CLAIMS

What is claimed is:

1. A method for security screening of electronic devices, comprising:

detecting an identifier from an electronic device;

querying a database with said identifier for information about said electronic device; and

responsive to receiving said information about said electronic device from said database, comparing at least one real-time scanned characteristic of said electronic device with said information, wherein if said at least one real-time scanned characteristic and said information match, then the electronic device is considered secure.

2. The method of claim 1 for security screening wherein detecting an identifier from an electronic device further comprises:

transmitting a radio frequency signal within a particular area for detecting said electronic device; and

reading said identifier from said electronic device broadcast from an antenna attached to a memory of said electronic device.

3. The method of claim 1 for security screening wherein querying a database further comprises:

querying said database with said identifier for information comprising physical characteristics of said electronic device.

4. The method of claim 1 for security screening wherein querying a database further comprises:

querying said database with said embedded identifier for information comprising an x-ray overlay of said electronic device.

5. The method of claim 1 for security screening wherein comparing at least one real-time scanned characteristic of said electronic device with said information further comprises:

scanning a three-dimensional image of said electronic device to attain a density signature for a plurality of components of said electronic device; and

comparing said density signature of said three-dimensional image with a previously recorded density signature returned with said information for said electronic device.

6. The method of claim 1 for security screening wherein comparing at least one real-time scanned characteristic of said electronic device with said information further comprises:

tracing a schematic figure of a plurality of components of said electronic device from a real-time x-ray scan; and

comparing said schematic figure of said plurality of components with a previously recorded schematic figure returned with said information for said electronic device.

7. The method of claim 1 for security screening wherein comparing at least one real-time scanned characteristic of said electronic device with said information further comprises:

comparing a real-time x-ray scan of said electronic device with a previously recorded x-ray scan returned with said information for said electronic device.

8. The method of claim 1 for security screening further comprising:

detecting a second identifier for a component of said electronic device; and

querying said database with said second identifier for second information about said component;

responsive to receiving said second information about said component from said database layered with said information for said electronic device, comparing at least one real-time scanned characteristic of said electronic device and said component with said layered information; and

responsive to receiving said second information about said component from said database separate from said information for said electronic device, comparing at least one real-time scanned characteristic of said component with said second information for said component.

9. The method of claim 1 for security screening further comprising:

determining whether said electronic device is properly positioned for scanning; and

responsive to detecting that said electronic device is not properly positioned for scanning, triggering an alert signal that an electronic device is not properly scannable.

10. The method of claim 1 for security screening, wherein querying a database with said identifier for information about said electronic device further comprises:

querying said database with said identifier via a network.

11. A system for security screening of electronic devices, comprising:

a screening system;

an identification reader connected to said screening system for reading an identifier from an electronic device within a security check area;

said screening system further comprising:

querying means for querying a database with said identifier for information about said electronic device; and

comparative means for comparing at least one real-time scanned characteristic of said electronic device with said information, responsive to receiving said information about said electronic device, wherein if said at

least one real-time scanned characteristic and said information match, then the electronic device is considered consistent and secure.

12. The system of claim 11 for security screening wherein said identification reader further comprises:

means for transmitting a radio frequency signal within a particular area for detecting said electronic device; and

means for reading said identifier from said electronic device broadcast from an antenna attached to a memory of said electronic device.

13. The system of claim 11 for security screening wherein said querying means further comprises:

means for querying said database with said identifier for information comprising physical characteristics of said electronic device.

14. The system of claim 11 for security screening wherein said querying means further comprises:

means for querying said database with said identifier for information comprising an x-ray overlay of said electronic device.

15. The system of claim 11 for security screening wherein said comparative means further comprises

means for scanning a three-dimensional image of said electronic device to attain a density signature for a plurality of components of said electronic device; and

means for comparing said density signature of said three-dimensional image with a previously recorded density signature returned with said information for said electronic device.

16. The system of claim 11 for security screening wherein said comparative means further comprises:

means for tracing a schematic figure of a plurality of components of said electronic device from a real-time x-ray scan; and

means for comparing said schematic figure of said plurality of components with a previously recorded schematic figure returned with said information for said electronic device.

17. The system of claim 11 for security screening wherein said comparative means further comprises:

means for comparing a real-time x-ray scan of said electronic device with a previously recorded x-ray scan returned with said information for said electronic device.

18. The method of claim 11 for security screening, said screening system further comprising:

means for detecting a second identifier for a component of said electronic device; and

means for querying said database via said network with said second identifier for second information about said component;

means, responsive to receiving said second information about said component from said database layered with said information for said electronic device, for comparing at least one real-time scanned characteristic of said electronic device and said component with said layered information; and

means, responsive to receiving said second information about said component from said database separate from said information for said electronic device, for comparing at least one real-time scanned characteristic of said component with said second information for said component.

19. The system of claim 11 for security screening, said screening system further comprising:

means for determining whether said electronic device is properly positioned for scanning; and

means, responsive to detecting that said electronic device is not properly positioned for scanning, for triggering an alert signal that an electronic device is not properly scannable.

20. The system of claim 11 for security screening wherein said screening system is communicatively connected to a network.

21. A computer program product stored on a computer operable medium for security screening of electronic devices, comprising:

means for detecting an identifier from an electronic device;

means for querying a database with said identifier for information about said electronic device; and

means, responsive to receiving said information about said electronic device, for comparing at least one real-time scanned characteristic of said electronic device with said information, wherein if said at least one real-time scanned characteristic and said information match, then the electronic device is considered secure.

22. The computer program product of claim 21 for security screening wherein said means for detecting an identifier from an electronic device further comprises:

means for transmitting a radio frequency signal within a particular area for detecting said electronic device; and

means for reading said identifier from said electronic device broadcast from an antenna attached to a memory of said electronic device.

23. The computer program product of claim 21 for security screening wherein said means for querying a database further comprises:

means for querying said database with said identifier for information comprising physical

characteristics of said electronic device.

24. The computer program product of claim 21 for security screening wherein said means for querying a database further comprises:

means for querying said database with said identifier for information comprising an x-ray overlay of said electronic device.

25. The computer program product of claim 21 for security screening wherein said means for comparing at least one real-time scanned characteristic of said electronic device with said information further comprises:

means for scanning a three-dimensional image of said electronic device to attain a density signature for a plurality of components of said electronic device; and

means for comparing said density signature of said three-dimensional image with a previously recorded density signature returned with said information for said electronic device.

26. The computer program product of claim 21 for security screening wherein said means for comparing at least one real-time scanned characteristic of said electronic device with said information further comprises:

means for tracing a schematic figure of a plurality of components of said electronic device from a real-time x-ray scan; and

means for comparing said schematic figure of said plurality of components with a previously recorded schematic figure returned with said information for said electronic device.

27. The computer program product of claim 21 for security screening wherein said means for comparing at least one real-time characteristic of said electronic device with said information further comprises:

means for comparing a real-time x-ray scan of said electronic device with a previously recorded x-ray scan returned with said information for said electronic device.

28. The computer program product of claim 21 for security screening further comprising:

means for determining whether said electronic device is properly positioned for scanning; and

means responsive to detecting that said electronic device is not properly positioned for scanning, for triggering an alert signal that an electronic device is not properly scannable.

29. A method for facilitating secure screening of electronic devices comprising:

receiving a request for information about an electronic device identified by a unique identifier;

searching a database for said unique identifier; and

responsive to locating information for said unique identifier in said database, returning said information formatted according to said request, such that an security screening system requesting said information is enabled to determine whether said electronic device is secure by matching said information to a real-time scanned characteristics of said electronic device.

30. The method according to claim 29 for facilitating secure screening of electronic devices further comprising:

receiving a request for information about an added component of said electronic device by a unique component identifier, wherein said added component is in additional to an original configuration of said electronic device;

searching said database for said unique component identifier; and

layering said information for said unique component identifier with said information for said electronic device, such that said information returned to said security screening device is a composite representing a current configuration of said electronic device.